Section3Math623

Monday, August 24, 2020 5:01 PM

Section3Math623

Section 3: Integral Domains and Fields

HW p. 10 # 1-10 at the end of the notes

Suppose we are asked to solve the equation

$$x^2 - 6x + 8 = 0$$

over the real numbers $\mathbb{R}$.

Over $\mathbb{R}$, $a \cdot b = 0$ only when $a = 0$ or $b = 0$.

Hence, we solve this quadratic equation as follows:

$$\begin{gathered} x^2 - 6x + 8 = 0 \\ (x-2)(x-4) = 0 \\ x - 2 = 0 \text{ or } x - 4 = 0 \\ x = 2, \; x = 4 \end{gathered}$$

However, suppose we are asked to solve the equation

$$x^2 - 6x + 8 = 0$$

over Z_{12}. Since $x^2 - 6x + 8 = (x-2)(x-4)$, $x = 2$ and $x = 4$ are solutions. However, $x = 8$ is a solution since

$$(x-2)(x-4) = (8-2)(8-4) = 6 \cdot 4 = 24 = 24 \,(\text{mod}\, 12) = 0$$

More than 2 solutions exist because 6 and 4 are *zero divisors*. That is, $6 \cdot 4 = 0$ in Z_{12} even though $6 \neq 0$ and $4 \neq 0$.

Definition 3.1: If a and b are two non-zero elements in a ring R such that $ab = 0$, then a and b are *divisors of zero* (or *zero divisors*).

For example, in Z_{10}, 2, 4, 5, 6, and 8 are zero divisors since

$$\begin{aligned} 2 \cdot 5 &= 10 \,(\text{mod } 10) = 0, & 4 \cdot 5 &= 20 \,(\text{mod } 10) = 0, \\ 5 \cdot 6 &= 30 \,(\text{mod } 10) = 0, & 5 \cdot 8 &= 40 \,(\text{mod } 10) = 0 \end{aligned}$$

Theorem 3.2: In the ring Z_m, the divisors of zero are precisely the non-zero elements that are not relatively prime to *m*, that is, *x* is a divisor of zero if $\gcd(x,m) > 1$.

Proof: Let $x \in Z_m$, $x \neq 0$ and suppose that $\gcd(x,m) = d > 1$. Then $d \mid x$ or $x = kd$ for some non-zero integer *x*. Also, $d \mid m$ or $m = ld$ for some non-zero integer *l*. Now

$$xl = k\,d\,l = k\,l\,d = km \underset{\text{mod}\,m}{=} 0.$$

Thus, *x* is a zero divisor if $\gcd(x,m) > 1$. Now, if $\gcd(x,m) = 1$, then if *x* is a zero divisor, there exists an $s \in Z_m$ where

$$xs \equiv 0 \,(\text{mod}\, m).$$

In Z_m, if $xs \equiv 0 \,(\text{mod}\, m)$, then $m \mid (xs - 0)$ or $m \mid xs$. Since $\gcd(x,m) = 1$, $m \mid s$ or $m \mid (s - 0)$. Thus $s \equiv 0 \,(\text{mod}\, m)$ or $s = 0$ in Z_m.

∎

Corollary to Theorem 3.2: If *p* is prime, then $\gcd(x,p) = 1$ for all non-zero $x \in Z_p$. Thus, there can be no divisors of zero.

Example 1: Find all solutions of $x^2 + 2x + 5 = 0$ in Z_8.

Solution: We are looking for values of $x \in Z_8 = \{0,1,2,3,4,5,6,7\}$ where $x^2 + 2x + 5 = 0$. These values are found by testing all the values in Z_8 for *x*. Substituting in, we obtain

x^2+2x+5

$$x = 0 \Rightarrow (0)^2 + 2(0) + 5 = 5 \neq 0$$

$$x = 1 \Rightarrow (1)^2 + 2(1) + 5 = 8 \underset{\text{mod}\,8}{=} 0$$

$$x = 2 \Rightarrow (2)^2 + 2(2) + 5 = 13 \underset{\text{mod}\,8}{=} 5 \neq 0$$

$$x = 3 \Rightarrow (3)^2 + 2(3) + 5 = 20 \underset{\text{mod}\,8}{=} 4 \neq 0$$

$$x = 4 \Rightarrow (4)^2 + 2(4) + 5 = 29 \underset{\text{mod}\,8}{=} 5 \neq 0$$

$$x = 5 \Rightarrow (5)^2 + 2(5) + 5 = 40 \underset{\text{mod}\,8}{=} 0$$

$$x = 6 \Rightarrow (6)^2 + 2(6) + 5 = 53 \underset{\text{mod}\,8}{=} 5 \neq 0$$

$$x = 7 \Rightarrow (7)^2 + 2(7) + 5 = 68 \underset{\text{mod}\,8}{=} 4 \neq 0$$

Thus, $x = 1$ and $x = 5$ are solutions.

∎

Cancellation Laws

Let R be a ring, and let $a, b, c \in R$. The left multiplicative cancellation laws hold in R if $ab = ac$ with $a \neq 0$ implies $b = c$. The right multiplicative cancellation laws hold in R if $ba = ca$ with $a \neq 0$ implies $b = c$.

Theorem 3.3: The cancellation laws hold in a ring R if an only if R has no zero divisors.

Proof: $\Rightarrow$ Suppose both the left and right cancellation laws hold and suppose

$$ab = 0.$$

If $a \neq 0$, then we can write

$$ab = 0 = a\,0$$

Since

$$\cancel{a}b = \cancel{a}\,0,$$

we can use the left cancellation law and see that $b = 0$. If $b \neq 0$, then we can write

$$ab = 0 = 0\,b$$

Since

$$a\cancel{b} = 0\cancel{b},$$

we can use the right cancellation law and see that $a = 0$. Hence, there are no zero divisors.

$\Leftarrow$ Now, suppose that R has no zero divisors. Suppose for $a \neq 0$ that

$$ab = ac$$

Since R is a ring, the addition inverse of ac, $-ac$, exists. Hence we have

$$ab - ac = 0$$

or

$$a(b - c) = 0.$$

Since $a \neq 0$ and R has no zero divisors, we must have

$$b - c = 0$$

or $b = c$. The right cancellation law follows similarly.

Definition 3.4: An *integral domain* D is a commutative ring with unity $1 \neq 0$ that contains no zero divisors.

Examples of Integral Domains

The integers Z, the integers modulo p, Z_p, where p is prime, and the real numbers R, are all examples of integral domains.

Examples of Rings that are not Integral Domains.

1. Z_n if n is not prime. For example, Z_{12} has zero divisors. For example, $4 \cdot 6 = 24 \underset{\text{mod}12}{\equiv} 0$.

2. $Z \times Z$ is not an integral domain. For example, $(r,0),(0,s) \in Z \times Z$, where $r \neq 0$, $s \neq 0$. However, $(r,0) \times (0,s) = (r \cdot 0, 0 \cdot s) = (0,0)$.

3. $M_2(Z)$ is the set of 2×2 matrices with integer entries.
$$\begin{bmatrix} 1 & 2 \\ 2 & 4 \end{bmatrix}\begin{bmatrix} -2 & -2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

4. $2Z = \{\ldots,-8,-6,-4,-2,0,2,4,6,8,\ldots\}$ is not an integral domain. $2Z$ has no zero divisors but it does not have the unity element since $1 \notin 2Z$.

Theorem 3.5: Every field F is an integral domain.

Proof:

By definition, a field is a commutative ring and has the unity element $1 \in F$

To show F has no zero divisors, suppose we have $a, b \in F$, $a \neq 0$ where

$$ab = 0 \quad \left(\begin{array}{c}\text{want to show} \\ b = 0\end{array}\right)$$

Since F is a field, then if $a \neq 0$, a^{-1} exists!

$$ab = 0$$
$$a^{-1} \cdot (a\,b) = a^{-1} \cdot 0$$
$$(a^{-1} \cdot a) b = 0$$
$$1 \cdot b = 0$$
$$b = 0$$

Hence, there are no zero divisors and F is an integral domain!

Page 6

Monday, August 24, 2020 5:02 PM

a $\mathbb{Z}_p$, p is a prime (example of a finite integral domain which is a field)

Theorem 3.6: Every finite integral domain D is a field.

Proof: Let $0, 1, a_1, a_2, \ldots, a_n$ be D's elements. We need to show for each non-zero $a \in D$, there exists $b \in D$ where $ab = 1$ (we want to show every non-zero element has a multiplicative inverse). Consider the non-zero elements of D

$$1, a_1, a_2, \ldots, a_n \qquad *$$

and consider the list of elements

$$a \cdot 1, aa_1, aa_2, \ldots, aa_n \qquad **$$

Note: Integers $\mathbb{Z}$ is an example of an infinite integral domain that is not a field

Note each $aa_i \neq 0$ since D is an integral domain and has no zero divisors. Also, all of the elements of * are distinct for if

$$aa_i = aa_j$$

Then,

$$a_i = a_j$$

by the left cancellation law. Hence, * and ** are just the same elements reordered. One of the elements in ** equals 1 in *. That is, either

$$a \cdot 1 = 1,$$

which implies $a = 1$ and a is its own multiplicative inverse or

$$aa_i = 1$$

and a_i is the multiplicative inverse of a. Thus, each arbitrary a in D has a multiplicative inverse and D is a field.

∎

Note: For a ring R, if $a \in R$ and $n \in Z^+$, then

$$na = \underbrace{a + a + a + \ldots a}_{n \text{ times}}$$

Definition 3.7: For a ring *R*, if there is a positive integer where $na = 0$ for all $a \in R$ for all $a \in R$, then the smallest such positive integer where this is true is called the *characteristic* of the ring. If no such positive integer exists, then *R* is of characteristic 0.

Example 1: What is the characteristic of Z_n?

Solution:

∎

Example 2: What is the characteristic of Z, Q, $\mathbb{R}$, and $\mathbb{C}$?

Solution:

∎

Theorem 3.8: Let *R* be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in Z^+$, then *R* has characteristic 0. If $n \cdot 1 = 0$ for some $n \in Z^+$, then the smallest such positive integer *n* is the characteristic of *R*.

Proof: If $n \cdot 1 \neq 0$ for all $n \in Z^+$, then we surely cannot have $n \cdot a = 0$ for all $a \in R$ for some positive integer *n*. Hence, by Definition 3, *R* has characteristic 0.

Now, suppose there is a positive integer *n* such that $n \cdot 1 = 0$. Then, for any $a \in R$, we have

$$na = \underbrace{a + a + a + \ldots a}_{n \text{ times}} = a\,(\underbrace{1 + 1 + 1 + \ldots 1}_{n \text{ times}}) = a\,(n \cdot 1) = a\,(0) = 0$$

Hence, by Definition 3, the result follows.

Example 3: What is the characteristic of $Z \times Z$?

Solution:

Example 4: What is the characteristic of Z_{10}?

Solution:

Example 5: What is the characteristic of $5Z$?

Solution:

Example 6: What is the characteristic of $Z_3 \times Z_2$?

Solution:

Example 7: What is the characteristic of $Z_3 \times 5Z$?

Solution:

$\blacksquare$

Recall that the binomial theorem say that

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}a^n$$

where $\binom{n}{r} = \dfrac{n!}{r!(n-r)!}$. This fact can be useful in polynomial expansion.

Example 8: If R is a commutative ring with unity with characteristic 4, compute and simplify

$$(a+b)^8 \text{ where } a,\ b \in R.$$

Solution: Recall that the binomial theorem says that

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n \text{ where } \binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Hence,

$$\begin{aligned}
(a+b)^8 &= \binom{8}{0}a^8 + \binom{8}{1}a^8b + \binom{8}{2}a^6b^2 + \binom{8}{3}a^5b^3 + \binom{8}{4}a^4b^4 + \binom{8}{5}a^3b^5 + \binom{8}{6}a^2b^6 + \binom{8}{7}ab^7 + \binom{8}{8}b^8 \\
&= a^8 + 8a^7b + 28a^6b^2 + 56a^5b^3 + 70a^4b^4 + 56a^3b^5 + 28a^2b^6 + 8ab^7 + b^8 \\
&= a^8 + 4(2a^7b) + 4(7a^6b^2) + 4(14a^5b^3) + 68a^4b^4 + 2a^4b^4 + 4(14a^3b^5) + 4(7a^2b^6) + 4(2ab^7) + b^8 \\
&= a^8 + 0 + 0 + 0 + 4(17a^4b^4) + 2a^4b^4 + 0 + 0 + 0 + b^8 \\
&= a^8 + 0 + 2a^4b^4 + b^8 \\
&\boxed{= a^8 + 2a^4b^4 + b^8}
\end{aligned}$$

$\blacksquare$

Exercises

1. Find all solutions to the following equations.
   a. $x^3 - 2x^2 - 3x = 0$ in Z_{12}.
   b. The equation $3x = 2$ in the field Z_{11}.
   c. Find the solutions of $x^2 + 2x + 2 = 0$ in Z_6.
   d. Find the solutions of $x^2 + 2x + 4 = 0$ in Z_6.

2. Find the characteristic of the given ring.
   a. $3Z$
   b. $Z \times Z$
   c. $Z_3 \times Z_3$
   d. $Z_3 \times Z_4$
   e. $Z_6 \times Z_{15}$

3. Let *R* be a commutative ring with unity of characteristic 4. Compute and simplify $(a+b)^4$ for $a, b \in R$.

4. Let *R* be a commutative ring with unity of characteristic 5. Compute and simplify $(a+b)^5$ for $a, b \in R$.

5. Let *R* be a commutative ring with unity of characteristic 3. Compute and simplify $(a+b)^9$ for $a, b \in R$.

6. Let *R* be a commutative ring with unity of characteristic 3. Compute and simplify $(a+b)^6$ for $a, b \in R$.

7. Show that the matrix $\begin{bmatrix} 2 & 4 \\ 4 & 8 \end{bmatrix}$ is a zero divisor in $M_2(Z)$.

8. Prove that a unit in a commutative ring cannot be a zero divisor.

9. An element of a ring *R* is idempotent if $a^2 = a$. Show that a division ring contains exactly two idempotent elements.

10. Show that the characteristic of an integral domain *D* must either 0 or a prime *p*. Hint: If the characteristic of *D* is a composite number *mn*, consider $(m \cdot 1)(n \cdot 1)$ in *D*.